INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 07:20 UTC

Inside a malicious infrastructure delivering EtherRAT, phishing pages, and malicious software

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0479
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Various, end users targeted via phishing and malware delivery; Windows systems implied by registry modification capability
Published	2026-06-15
Discovery Source	Gemini

Executive Summary

Threat hunters have identified a large-scale shared malicious infrastructure distributing EtherRAT, phishing pages, and additional malware across multiple concurrent campaigns. The infrastructure appears to operate as a malware-as-a-service or bulletproof hosting platform, assigning distinct delivery endpoints per campaign and targeting Windows end users through multi-stage phishing lures followed by RAT deployment. Organizations face risk of data exfiltration, persistent remote access, and credential theft, with the shared-platform model suggesting organized, ongoing threat activity rather than isolated incidents.

Technical Analysis

This campaign centers on a shared malicious infrastructure delivering EtherRAT, a remote access trojan with capabilities including arbitrary JavaScript execution, file system read/write operations, Windows registry modification (CWE-269: Improper Privilege Management; T1112 Modify Registry), and data exfiltration over command-and-control channels (T1041). The delivery chain begins with phishing lures (T1566) that redirect victims to actor-controlled pages (CWE-601: URL Redirection to Untrusted Site), then retrieve and execute payloads via ingress tool transfer (T1105; CWE-494: Download of Code Without Integrity Check). JavaScript execution capability maps to T1059.007 (Command and Scripting Interpreter: JavaScript). Infrastructure acquisition aligns with T1583.008 (Acquire Infrastructure: Malvertising) and T1588.001 (Obtain Capabilities: Malware), consistent with a malware-as-a-service or bulletproof hosting model with per-campaign URL endpoint assignment. CWE references: CWE-269, CWE-601, CWE-494, CWE-78.

Action Checklist

1. Step 1: Containment. Identify and block known malicious infrastructure at the perimeter. Identify and isolate any Windows endpoints exhibiting outbound connections to unfamiliar or newly registered domains. Enforce DNS filtering to block resolution of domains associated with this campaign. Apply NIST AC-4 (Information Flow Enforcement) to restrict unauthorized outbound data flows from endpoints.
2. Step 2: Detection. Review endpoint and network logs for the following behavioral indicators: outbound JavaScript execution from user-context processes, registry modification events outside change windows (monitor HKCU and HKLM run keys), file writes to %APPDATA% or %TEMP% by browser or document-handling processes, and HTTP/S connections to infrastructure domains not in your approved list. Query EDR telemetry for T1112 (registry mod), T1059.007 (JS interpreter invocation), and T1041 (data exfil). Enable AU-2 (Event Logging) for process creation, network connection, and registry modification event classes if not already active. Apply CIS 8.2 (Collect Audit Logs) to confirm logging is enabled across all Windows endpoints.
3. Step 3: Eradication. On confirmed-compromised endpoints, terminate EtherRAT processes, remove persistence entries from registry run keys and startup locations, and delete dropped payloads from file system. Block phishing redirect URLs at the email gateway and web proxy. Remove or quarantine any files with unverified integrity matching known malware delivery patterns. Apply NIST SI-3 class controls for malicious code protection if mapped in your environment.
4. Step 4: Recovery. After eradication, rotate credentials for any accounts that authenticated on affected endpoints, prioritizing service accounts and privileged users. Re-image endpoints where full eradication confidence is low. Validate that registry run keys, startup folders, and scheduled tasks are clean. Monitor reinstated endpoints for 72 hours using EDR behavioral analytics. Apply NIST AC-2 (Account Management) to review and revoke any accounts whose sessions may have been harvested.
5. Step 5: Post-Incident. Audit phishing awareness training currency and simulate a phishing exercise targeting the delivery method observed here. Review email gateway and DNS filtering configurations for gaps that allowed initial lure delivery. Implement or tune detection rules for T1566 (phishing), T1105 (ingress tool transfer), and T1059.007 (JavaScript execution); see Detection Guidance above for specific behavioral indicators and EDR queries. Enforce NIST AC-6 (Least Privilege) to limit the blast radius of any future RAT deployment. Apply CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure endpoint agents and email security tooling are current.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and data protection officer immediately if EtherRAT C2 activity is confirmed on any endpoint storing PII, PHI, or financial data, or if credential harvesting scope extends to privileged or service accounts, as this may trigger breach notification obligations under GDPR, HIPAA, or applicable state data protection law.

Recovery Notes	After eradication, re-image any endpoint where EtherRAT process execution was confirmed rather than relying solely on registry and file cleanup, as the RAT's persistence mechanism and potential for kernel-level hooks make partial remediation unreliable. Validate all reinstated endpoints against a known-good Autoruns baseline and monitor Sysmon Event ID 1, 3, and 13 streams for recurrence of EtherRAT execution indicators for a minimum of 72 hours before returning to normal operations. Conduct a DNS and email gateway IOC review weekly for 30 days post-incident, as bulletproof hosting platforms supporting this campaign type routinely rotate infrastructure domains to reinfect imperfectly remediated environments.
Forensic Artifacts	Windows Registry run key exports — HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run — for EtherRAT persistence entries written during initial compromise; capture via `reg export` before any eradication action | RAM image (WinPmem/DumpIt) from compromised Windows endpoints preserving in-memory EtherRAT process, embedded C2 configuration, active socket handles, and credential material harvested before session termination or isolation | Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connect) logs showing JavaScript interpreter process (wscript.exe, mshta.exe, cscript.exe) spawned under browser or email client parent with subsequent outbound TCP connections to campaign infrastructure domains | Browser and email client file write artifacts — specifically files dropped to %APPDATA%\Roaming\ and %TEMP%\ by chrome.exe, msedge.exe, or outlook.exe during the phishing lure interaction stage, recoverable via MFT ($MFT) analysis using Velociraptor or MFTECmd even if files were subsequently deleted | DNS resolver cache and query logs (`ipconfig /displaydns` output and DNS debug log at %SystemRoot%\System32\dns\dns.log if enabled) recording resolution of campaign infrastructure domains, establishing initial access timeline and full set of C2 and payload delivery hostnames contacted by the endpoint

Per-Action IR Details

Step 1: Containment — Block known malicious infrastructure at the perimeter immediately. Identify and isolate any Windows endpoints exhibiting outbound connections to unfamiliar or newly registered domains. Enforce DNS filtering to block resolution of domains associated with this campaign. Apply NIST AC-4 (Information Flow Enforcement) to restrict unauthorized outbound data flows from endpoints.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Export NetFlow or Windows Firewall logs and pipe through PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Windows Firewall With Advanced Security/Firewall' | Where-Object {$_.Message -match 'DROP'}`. Use Pi-hole or Windows DNS debug logging (`dnscmd /config /log`) to enumerate and block newly registered domains (WHOIS age < 30 days). Deploy free Quad9 DNS-over-HTTPS to enforce blocking without enterprise DNS appliances. Two-person team can work from a prioritized IOC list extracted from the campaign report.

Evidence: Before isolating any endpoint, capture: full RAM image using WinPmem or DumpIt to preserve EtherRAT in-memory process state and C2 socket handles; run `netstat -ano` and `Get-NetTCPConnection` to record all active outbound TCP sessions including EtherRAT C2 channel destinations; capture DNS cache via `ipconfig /displaydns` to surface recently resolved campaign infrastructure domains before isolation flushes live state; export Windows Firewall connection log (`%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`) for outbound connection history to newly registered domains.

Step 2: Detection — Review endpoint and network logs for the following behavioral indicators: outbound JavaScript execution from user-context processes, registry modification events outside change windows (monitor HKCU and HKLM run keys), file writes to %APPDATA% or %TEMP% by browser or

document-handling processes, and HTTP/S connections to infrastructure domains not in your approved list. Query EDR telemetry for T1112 (registry mod), T1059.007 (JS interpreter invocation), and T1041 (data exfil). Enable AU-2 (Event Logging) for process creation, network connection, and registry modification event classes if not already active. Apply CIS 8.2 (Collect Audit Logs) to confirm logging is enabled across all Windows endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (Process Create), Event ID 3 (Network Connect), Event ID 12/13 (Registry Create/Set) targeting HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent keys. Query with: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 13 -and $_.Message -match 'CurrentVersion\\Run'}`. Use free Sigma rule 'proc_creation_win_wscript_cscript_dropper' to detect wscript.exe or cscript.exe spawned under browser or document-handler parent processes delivering the JavaScript-stage phishing lure.

Evidence: This step is read-only analysis and does not alter live state, so volatile capture is not a prerequisite for the query phase itself. However, if any endpoint is selected for deep-dive analysis based on findings here, capture RAM and live connection state before proceeding. Key artifacts to query now: Sysmon Event ID 3 for outbound connections from wscript.exe, mshta.exe, or powershell.exe to campaign domains; Windows Security Event ID 4688 (Process Creation) with command-line auditing enabled filtering on wscript.exe or cscript.exe spawned by outlook.exe, chrome.exe, or msedge.exe; registry audit events at HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run for EtherRAT persistence entries; file system events for writes to %APPDATA%\Roaming\ or %TEMP%\ by browser processes, which is consistent with multi-stage phishing payload drops observed in this campaign.

Step 3: Eradication — On confirmed-compromised endpoints, terminate EtherRAT processes, remove persistence entries from registry run keys and startup locations (audit via D3-SICA: System Init Config Analysis), and delete dropped payloads from file system. Block phishing redirect URLs at the email gateway and web proxy. Remove or quarantine any files with unverified integrity matching known malware delivery patterns (D3-FMBV: File Magic Byte Verification). Apply NIST SI-3 class controls for malicious code protection if mapped in your environment.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.3 (Address Unauthorized Software)

Compensating: Use Autoruns (Sysinternals) to enumerate and remove EtherRAT persistence entries from all run key locations, scheduled tasks, and startup folders — filter by VirusTotal integration to flag unsigned or unrecognized entries. Delete payload files from %APPDATA%\Roaming\ and %TEMP%\ identified in Step 2 analysis. Scan remaining filesystem with ClamAV using updated signatures targeting known EtherRAT and associated dropper hashes from the campaign report. Verify file magic bytes of any .js, .exe, or .dll in user-writable directories do not mismatch declared extensions (common phishing dropper technique in this campaign).

Evidence: Before terminating EtherRAT processes or modifying registry keys: capture full RAM image (WinPmem/DumpIt) to preserve in-memory EtherRAT configuration including embedded C2 addresses, encryption keys, and operator-controlled parameters that are not written to disk; run `tasklist /v /fo csv` and `wmic process get name,processid,parentprocessid,commandline /format:csv` to record EtherRAT process tree and parent-child relationships before kill; export full registry hive for HKCU and HKLM run keys via `reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run C:\IR\runkeys_hkcu.reg` before deletion; document all files in %APPDATA%\Roaming\ and %TEMP%\ with hash values (`Get-FileHash -Algorithm SHA256`) before removal to support downstream threat intelligence and legal preservation requirements.

Step 4: Recovery — After eradication, rotate credentials for any accounts that authenticated on affected endpoints, prioritizing service accounts and privileged users (D3-CRO: Credential Rotation). Re-image endpoints where full eradication confidence is low. Validate that registry run keys, startup folders, and scheduled tasks are clean. Monitor reinstated endpoints for 72 hours using EDR behavioral analytics. Apply NIST AC-2 (Account Management) to review and revoke any accounts whose sessions may have been harvested.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Force credential rotation via `net user /domain` or local equivalent for all accounts with interactive logon history on compromised endpoints (query via `Get-WinEvent -LogName Security -Id 4624 | Where-Object {$_.Message -match "}`). For re-imaged endpoints, validate clean state by running Autoruns and Sysmon for 72 hours post-restoration, reviewing Event ID 13 (Registry Set) and Event ID 1 (Process Create) for recurrence of EtherRAT execution patterns. Use osquery scheduled query `SELECT * FROM startup_items` and `SELECT * FROM scheduled_tasks` to continuously validate persistence locations are clean on reinstated hosts.

Evidence: Before rotating credentials or re-imaging: export Windows Security Event Log for Event ID 4624 (Successful Logon), 4648 (Logon with Explicit Credentials), and 4776 (Credential Validation) to identify all accounts whose credentials were used on the compromised endpoint during the compromise window — EtherRAT has credential harvesting capability and this log set establishes the full blast radius; capture browser credential store locations (%APPDATA%\Local\Google\Chrome\User Data\Default\Login Data, equivalent for Edge) for forensic imaging before re-image destroys them; document all authenticated sessions via `query session` and `quser` before termination to establish scope for breach notification assessment.

Step 5: Post-Incident — Audit phishing awareness training currency and simulate a phishing exercise targeting the delivery method observed here. Review email gateway and DNS filtering configurations for gaps that allowed initial lure delivery. Implement or tune detection rules for T1566, T1105, and T1059.007. Enforce NIST AC-6 (Least Privilege) to limit the blast radius of any future RAT deployment. Apply CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure endpoint agents and email security tooling are current.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST AU-12 (Audit Record Generation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Build phishing simulation using GoPhish (free, open source) replicating the multi-stage lure pattern observed in this campaign — specifically a credential-harvesting redirect page followed by a JavaScript-based payload delivery stage. Write Sigma detection rule targeting wscript.exe or mshta.exe spawned from outlook.exe or browser processes with outbound network connections within 60 seconds of execution (indicative of this campaign's JS-dropper-to-EtherRAT chain). Publish IOCs (domains, file hashes, registry key names) to internal threat intel repository or share via MISP for cross-organization detection.

Evidence: This phase does not alter live host state; volatile capture is not required. Collect and preserve for lessons-learned: full timeline of DNS query logs showing when campaign domains were first resolved within the environment (to establish dwell time); email gateway logs showing original phishing lure delivery including sender infrastructure, subject lines, and attachment or link patterns specific to this campaign's multi-stage delivery chain; compiled IOC set (C2 domains, EtherRAT binary hashes, dropper JS file hashes, registry persistence key names and values) documented for detection rule tuning and future threat hunting hypotheses.

Detection Guidance

Focus detection on four behavioral clusters:

1. Registry modification: Monitor for writes to HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalents by non-administrative processes. EDR query: process_name NOT IN (approved_software_list) AND registry_key LIKE '%CurrentVersion\Run%'.

2. JavaScript execution outside browser context: Alert on wscript.exe, cscript.exe, or node.exe spawned by office productivity, PDF, or download-manager processes. MITRE T1059.007.

3. Ingress tool transfer: Detect file writes to %TEMP%, %APPDATA%, or %ProgramData% by browser or email client processes, followed within 60 seconds by process creation from the same path. T1105.

4. Exfiltration over C2: Baseline outbound connection volume per endpoint; consider alerting on sustained low-bandwidth HTTP/S sessions to newly registered or uncategorized domains that deviate from baseline per endpoint. T1041.

Phishing delivery indicators: Inspect email headers for mismatched reply-to and from domains, URL redirects through free hosting or URL-shortening services, and HTML attachment payloads. CWE-601 redirect chains often land on lookalike credential-harvest pages before payload delivery.

Recommended log sources: Windows Security Event Log (Event IDs 4657 registry modification, 4688 process creation with command line), Sysmon (Event IDs 1, 3, 13), EDR telemetry, DNS query logs, web proxy logs, and email gateway logs.

D3FEND countermeasures: D3-LAM (Local Account Monitoring) for post-compromise account activity; D3-SFA (System File Analysis) for tampered executables; D3-UAP (User Account Permissions) to confirm least-privilege enforcement.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`no specific IOCs provided in source data`	No authoritative IOC list was included in the raw data for this campaign; source material did not contain verified indicators. Operators should monitor threat intelligence feeds for EtherRAT infrastructure indicators as they are published.	LOW

Framework Mappings

MITRE-ATTACK

- **T1112** — Modify Registry
- **T1588.001** — Malware
- **T1105** — Ingress Tool Transfer
- **T1041** — Exfiltration Over C2 Channel

- **T1583.008** — Malvertising
- **T1566** — Phishing
- **T1059.007** — JavaScript

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **SI-10** — Information Input Validation
- **CM-7** — Least Functionality

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures
- **A03:2021** — Injection

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1112	Modify Registry	Defense-Evasion
T1588.001	Malware	Resource-Development

Technique ID	Technique Name	Tactic
T1105	Ingress Tool Transfer	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration
T1583.008	Malvertising	Resource-Development
T1566	Phishing	Initial-Access
T1059.007	JavaScript	Execution

Sources

Source	URL	Tier
What is Phishing? Types, Risks, and Protection Strategies - Fortinet	https://www.fortinet.com/resources/cyberglossary/phishing	T3
What is Phishing? | IBM	https://www.ibm.com/think/topics/phishing	T3
Malware, Phishing, and Ransomware - CISA	https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-ph...	T1
The Enterprise Guide to Phishing Attacks: Types & Defenses	https://www.adaptivesecurity.com/blog/the-enterprise-guide-to-phish...	T3
Cyber Security Awareness - What is it and why is it important?	https://www.dataguard.com/cyber-security/awareness/	T3

Generated 2026-06-16 07:20 UTC by TJS Security Command Center